

# Tesina: Integración de herramientas de seguridad para redes informáticas

Autores: Matías Pagano y Einar Felipe Lanfranco

Director: Francisco Javier Díaz

Codirectora: Paula Venosa

# Resumen

- Componentes a integrar
- Opciones analizadas y productos elegidos
- Integración
- Desarrollo
- Futuro
- Conclusiones

# Componentes a integrar

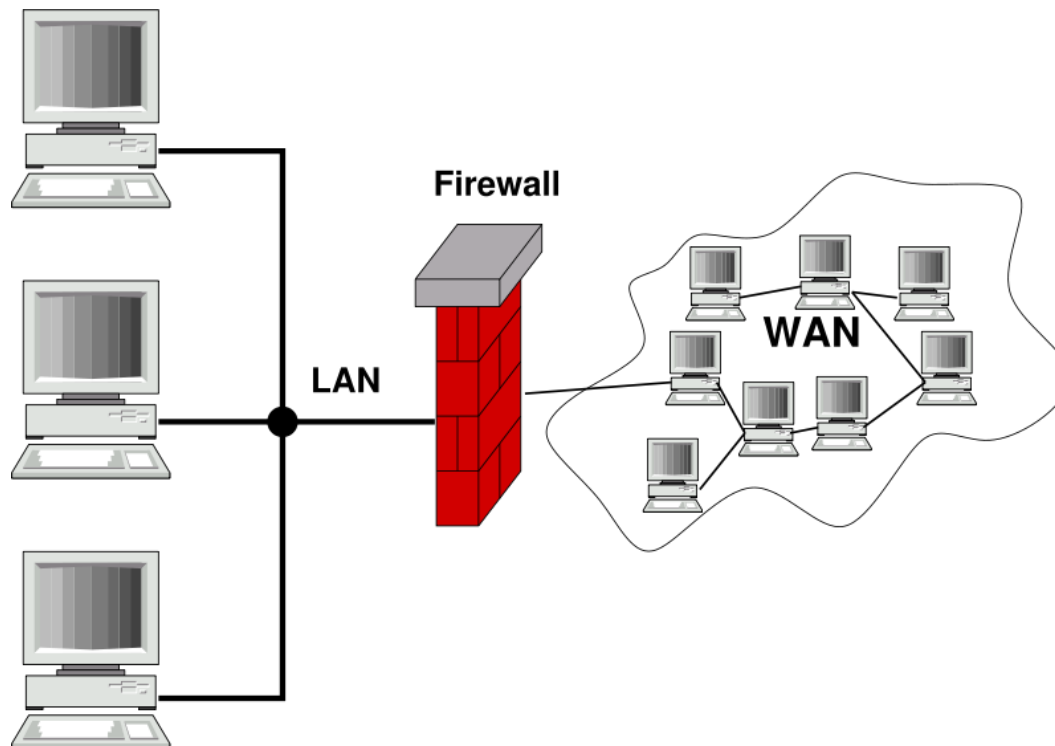


# Componentes a integrar



# Firewall

- ¿Qué es un firewall?
- Elemento que sirve para controlar las comunicaciones, permitiéndolas o prohibiéndolas, según las políticas definidas



# Firewall

- En que capas trabaja



# Componentes a integrar



- **¿Qué es un IDS?**

Aplicación diseñada para examinar tráfico de red y/o archivos de logs en busca de comportamiento sospechoso.

- **¿Qué hace?**

En su modo más simple de funcionamiento genera alertas.

- **¿Para qué sirve?**

Estas alertas permiten tomar las medidas necesarias para contrarrestar la actividad maliciosa o corregir los errores de configuración que se hayan detectado.

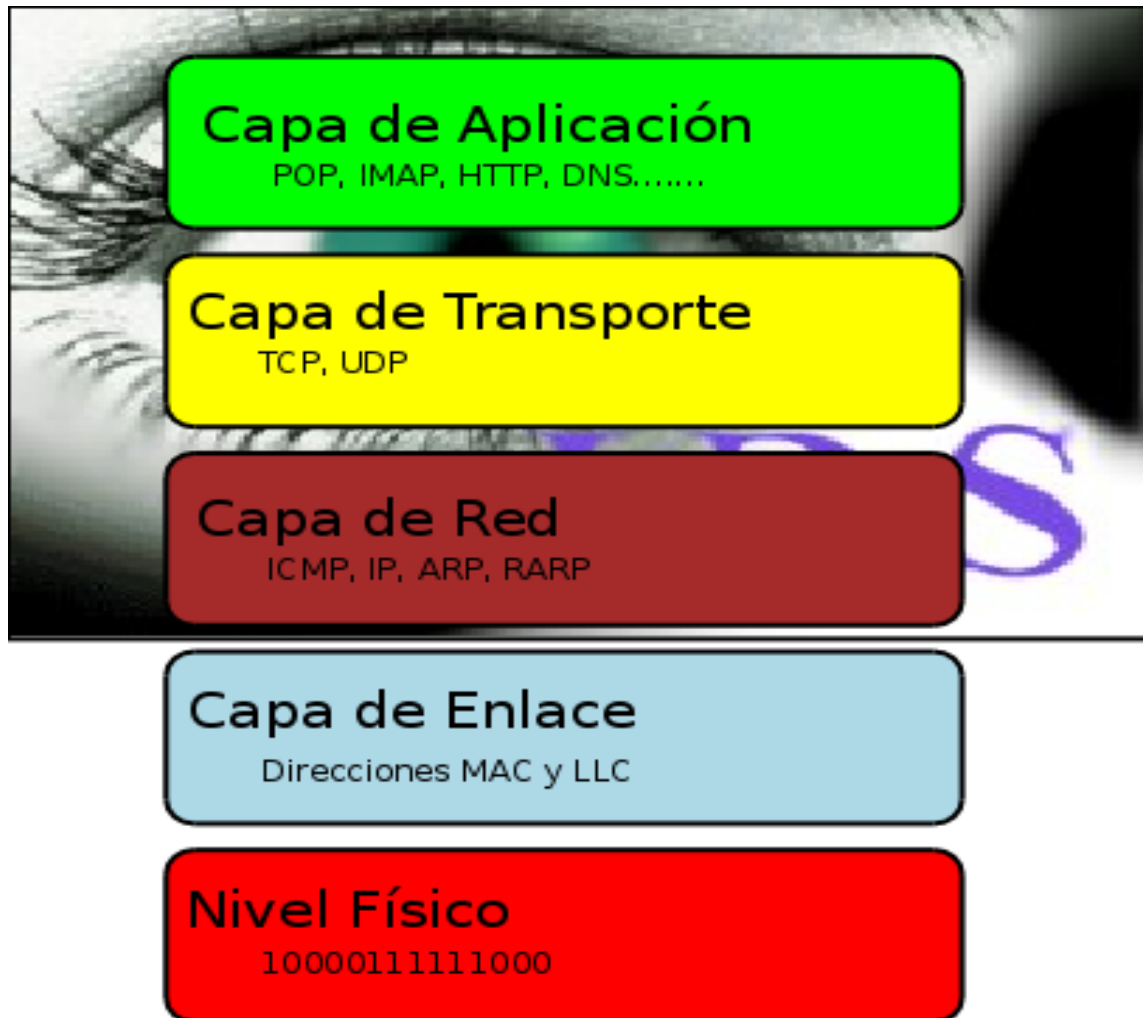


# IDS

- Si ya se tiene un firewall, para qué se necesita un IDS?
- Un sistema de detección de intrusiones funciona a manera de complemento del firewall.
- Es un mecanismo de control que nos sirve para monitorear qué pasa dentro de nuestro entorno, una vez que se supera la barrera impuesta por el firewall.

# IDS

- ¿En qué capas trabaja?



# Componentes a integrar

A 3D rendered hand holding a magnifying glass, focusing on a large green question mark. The scene is set within a circular frame. In the background, a person's eye is visible, looking towards the magnifying glass. The overall image conveys a sense of investigation or searching for answers.

**ESCANER DE  
VULNERABILIDADES**

# Escaner de Vulnerabilidades

- **¿Qué es?**

Un escaneador de vulnerabilidades es un programa diseñado para buscar fallas o debilidades en las aplicaciones o en su configuración.

- **¿Qué escanea?**

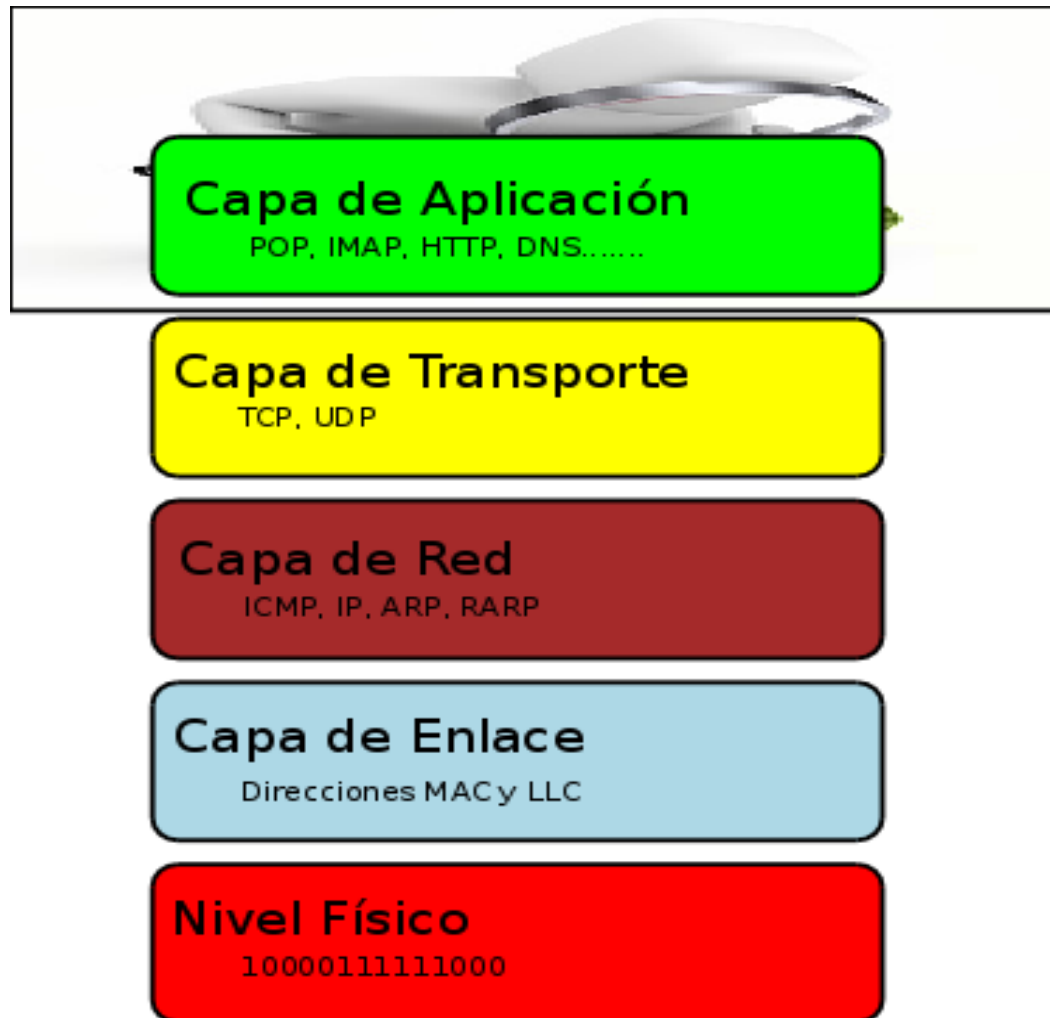
Típicamente el ambiente de búsqueda es un host, un grupo de hosts en particular o todos los hosts de una red o subred dada.

# Escaner de Vulnerabilidades

- **¿Cómo funciona?**
  - Busca direcciones IP activas
  - Intenta identificar los puertos abiertos
  - Intenta identificar qué sistema operativo y/o aplicaciones se están ejecutando
  - Finalmente intentará obtener la versión exacta de cada aplicación y cada sistema operativo para averiguar el nivel de actualización

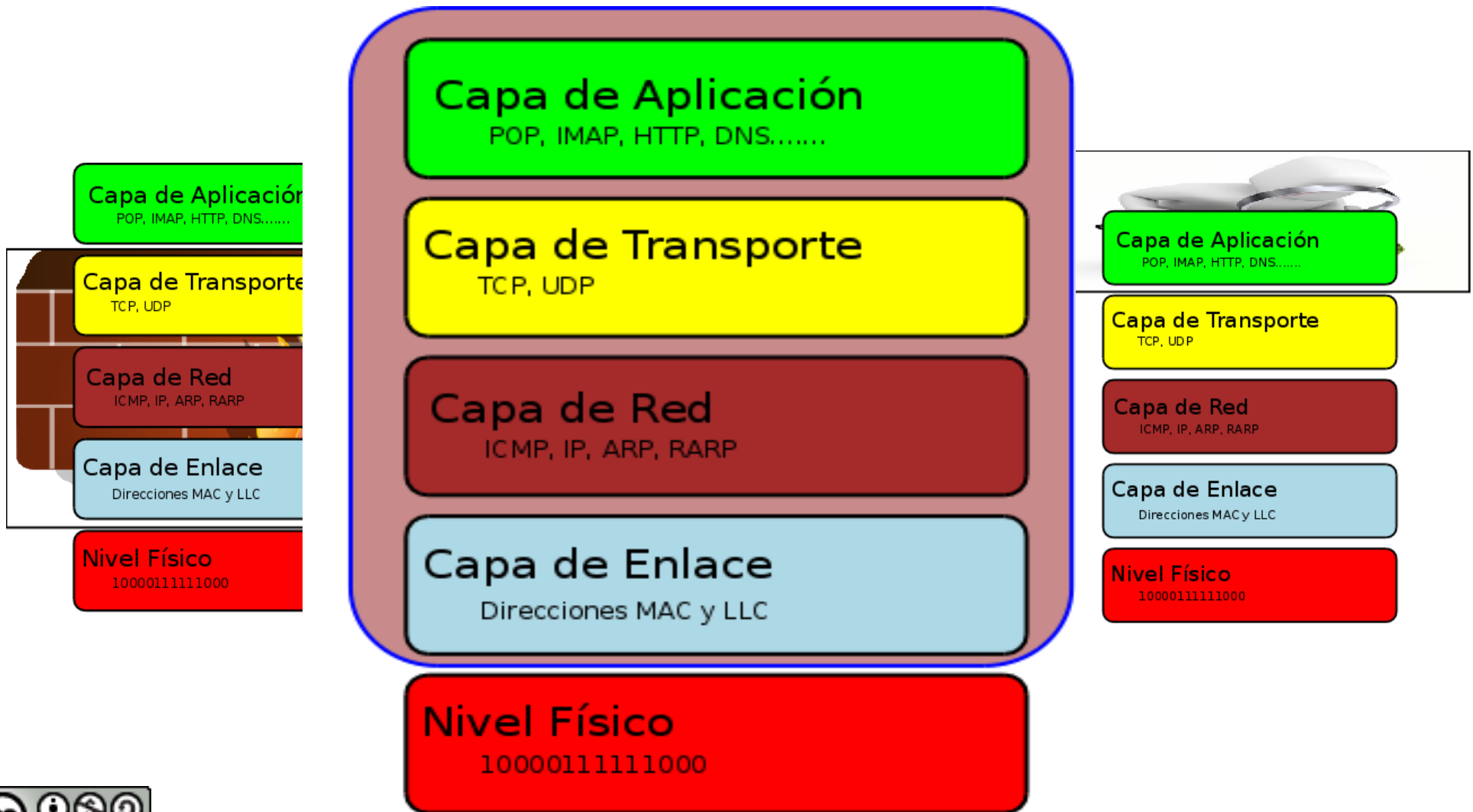
# Escaner de Vulnerabilidades

- ¿En qué capas trabaja?



# Resultado

- ¿En qué capas trabaja?



# Software a integrar

## Crterios de seleccin:

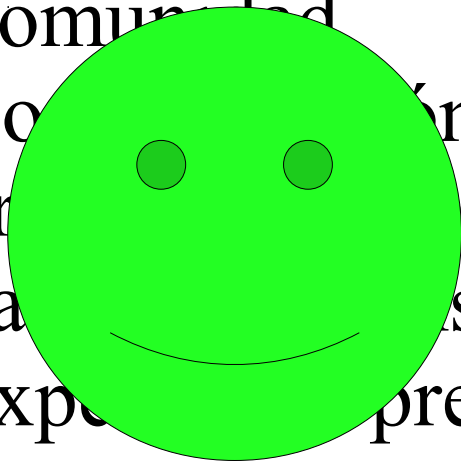
- La licencia con la que se distribuye el software.
- La comunidad que lo utiliza.
- La documentacin existente.
- Las pruebas realizadas cuando quisimos integrarlos.
- La facilidad de instalacin.
- La experiencia previa en el uso de los mismos.



# Elección de SO

## GNU/Linux

- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Precio
- ✓ Prácticidad
- ✓ Facilidad de instalación
- ✓ Experiencia previa



Debian



Ubuntu



Fedora



Gentoo



Mandriva



Suse

slackware  
linux

Slackware



PCLinuxOS

PCLinuxOS



Red Hat Enterprise Linux

## BSD

- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Precio
- ✓ Prácticidad
- ✓ Facilidad de instalación
- ✗ Experiencia previa



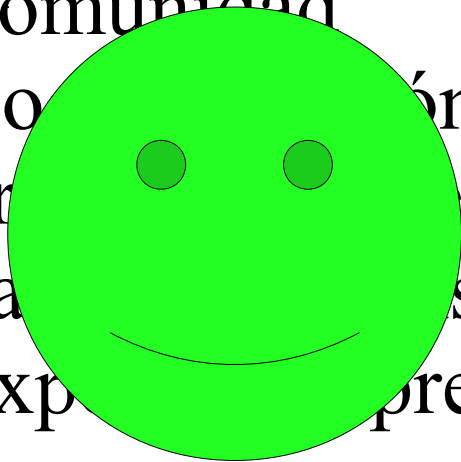
OpenDarwin



# Elección de FW

## Netfilter/iptables

- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Pruebas de integración
- ✓ Facilidad de instalación
- ✓ Experiencia previa



## PF/ BSD

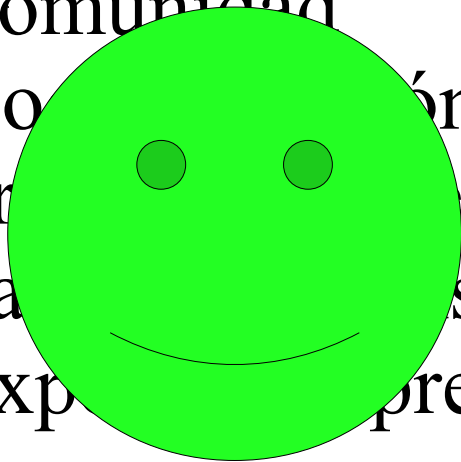
- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Pruebas de integración
- ✓ Facilidad de instalación
- ✗ Experiencia previa



# Elección de IDS

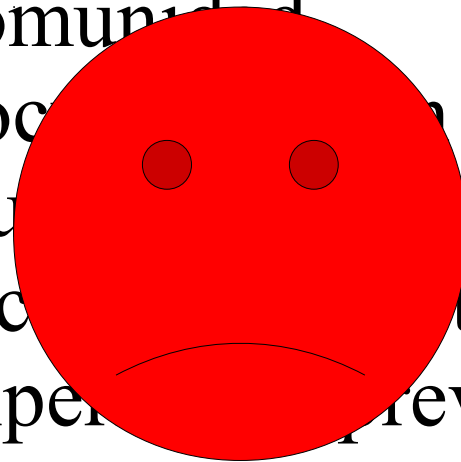
## SNORT

- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Pruebas de integración
- ✓ Fácil instalación
- ✓ Experiencia previa



## BRO - IDS

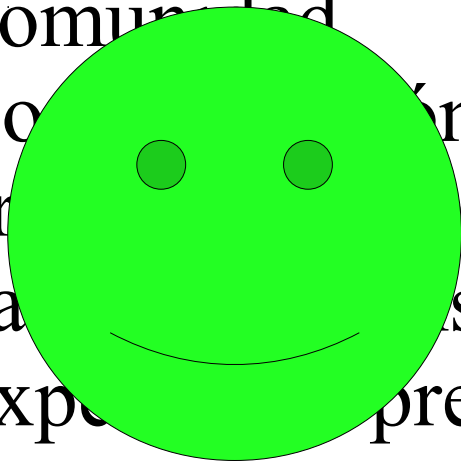
- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Pruebas de integración
- ✗ Fácil instalación
- ✓ Experiencia previa



# Elección de Escaner de Vuln.

## OpenVAS

- ✓ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Pruebas de integración
- ✓ Fácil instalación
- ✓ Experiencia previa



## Nessus

- ✗ Licencia
- ✓ Comunidad
- ✓ Documentación
- ✓ Pruebas de integración
- ✓ Fácil instalación
- ✓ Experiencia previa



# Opciones analizadas y productos elegidos



# Integrando

- Reglas Iptables:

```
# REGLAS PARA LIMPIAR EL FIREWALL
iptables -F TESIS;

#### REGLAS DEL SERVIDOR: Sitio Web Linti (163.10.10.13/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.13 -p TCP --dport 80 -m state --state NEW -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.13 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.13 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Distancia (163.10.10.21/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.21 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.21 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Lihuen (163.10.10.17/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.17 -p TCP --dport 7000 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.17 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.17 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Mail del LINTI (163.10.10.61/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 993 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.61 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#### REGLAS DEL SERVIDOR: Listas (163.10.10.22/255.255.255.255) ####
# TRAFICO ENTRANTE
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.22 -p TCP --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 0.0.0.0 -d 163.10.10.22 -p TCP --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 163.10.53.122 -d 163.10.10.22 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 163.10.33.64 -d 163.10.10.22 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A TESIS -s 163.10.20.0 -d 163.10.10.22 -p TCP --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```



# Integrando

- Alertas generadas por Snort:

```
[**] [1:469:3] ICMP PING NMAP [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
05/15-08:20:54.377357 10.3.16.107 -> 10.3.9.152  
ICMP TTL:57 TOS:0x0 ID:33363 Iplen:20 Dgmlen:28  
Type:8 Code:0 ID:22024 Seq:0 ECHO  
[Xref => http://www.whitehats.com/info/IDS162]  
  
[**] [122:1:0] (portscan) TCP Portscan [**]  
[Priority: 3]  
05/15-08:20:54.438127 10.3.16.107 -> 10.3.9.152  
PROTO:255 TTL:0 TOS:0x0 ID:0 Iplen:20 Dgmlen:157 DF  
  
[**] [1:1421:11] SNMP AgentX/tcp request [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
05/15-08:20:55.891333 10.3.16.107:41343 -> 10.3.9.152:705  
TCP TTL:53 TOS:0x0 ID:45579 Iplen:20 Dgmlen:44  
*****S* Seq: 0xC1DDAD5E Ack: 0x0 Win: 0xC00 TcpLen: 24  
TCP Options (1) => MSS: 1460  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012][Xref => http://www.securis  
  
[**] [1:1420:11] SNMP trap tcp [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
05/15-08:20:59.097292 10.3.16.107:41343 -> 10.3.9.152:162  
TCP TTL:48 TOS:0x0 ID:18580 Iplen:20 Dgmlen:44  
*****S* Seq: 0xC1DDAD5E Ack: 0x0 Win: 0x800 TcpLen: 24  
TCP Options (1) => MSS: 1460  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012][Xref => http://www.securis  
  
[**] [1:1418:11] SNMP request tcp [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
05/15-08:21:00.498347 10.3.16.107:41343 -> 10.3.9.152:161  
TCP TTL:56 TOS:0x0 ID:51164 Iplen:20 Dgmlen:44  
*****S* Seq: 0xC1DDAD5E Ack: 0x0 Win: 0x800 TcpLen: 24
```

# Integrando

- Reporte de escaneo de OpenVAS:

```
timestamps|||scan_start|Fri Dec 3 07:37:19 2010|
timestamps||163.10.10.109|host_start|Fri Dec 3 07:37:19 2010|
results|163.10.10|163.10.10.109|general/tcp|1.3.6.1.4.1.25623.1.0.90022|Log Message|No port for an ssh connect was found open.\nHence local security checks might not work.\n
results|163.10.10|163.10.10.109|ssh (22/tcp)|1.3.6.1.4.1.25623.1.0.50282|Log Message|\nThis script will, if given a userid/password or\nkey to the remote system, login to that system,\ndetermine the OS it is
running, and for supported\nsystems, extract the list of installed packages/rpms.\n\nRisk factor : None\n
results|163.10.10|163.10.10.109|general/tcp|1.3.6.1.4.1.25623.1.0.102002|Security Note|ICMP based OS fingerprint results: \n\nUnable to detect remote OS. No match found.\n\n\n
results|163.10.10|163.10.10.109|general/tcp|1.3.6.1.4.1.25623.1.0.90003|Log Message|\nThis script connects to SLAD on a remote host to fetch\nthe result from scripts started earlier.\nTo work properly, this
script requires to be provided\nwith a valid SSH login by means of an SSH key with pass.\nphrase if the SSH public key is passphrase-protected, or\na password to log in.\n
results|163.10.10|163.10.10.109|http (80/tcp)|1.3.6.1.4.1.25623.1.0.80110|Log Message|wapiti report filename is empty. that could mean that\nwrong version of wapiti is used or tmp dir is not accessible.\nMak
e sure to have wapiti 2.x as wapiti 1.x is not supported.\nIn short: check installation of wapiti and OpenVAS\n
results|163.10.10|163.10.10.109|general/tcp|1.3.6.1.4.1.25623.1.0.90002|Log Message|\nThis script connects to SLAD on a remote host to run\nremote scanners.\nTo work properly, this script requires to be prov
ided\nwith a valid SSH login by means of an SSH key with pass.\nphrase if the SSH public key is passphrase-protected, or\na password to log in.\n
results|163.10.10|163.10.10.109|general/tcp|1.3.6.1.4.1.25623.1.0.51662|Security Note|Here is the route from 163.10.20.60 to 163.10.10.109\n\n163.10.20.60\n163.10.20.1\n163.10.33.189\n163.10.33.54\n* * *\n16
3.10.10.109\n\n
results|163.10.10|163.10.10.109|http (80/tcp)|1.3.6.1.4.1.25623.1.0.80109|Log Message|w3af report filename is empty. that could mean that\nwrong version of w3af is used or tmp dir is not accessible.\nIn shor
t: check installation of w3af and OpenVAS\n
results|163.10.10|163.10.10.109|general/SMBClient|1.3.6.1.4.1.25623.1.0.90011|Log Message|Error getting SMB-Data -> CONNECTION TO 163.10.10.109 FAILED (ERROR NT_STATUS_UNSUCCESSFUL)\n
results|163.10.10|163.10.10.109|http (80/tcp)|1.3.6.1.4.1.25623.1.0.14260|Security Note|Here is the Nikto report:\nUnknown option: ask no\n\nCgidirs+ scan these CGI dirs: 'none', 'all', or values
like "/cgi/ /cgi-a/*"\n\n-dbcheck check database and other key files for syntax errors (cannot be abbreviated)\n-evasion+ ids evasion technique\n-Format+ save file (-o) format\n-
host+ target host\n-Help Extended help information\n-id+ host authentication to use, format is userid:password\n-list-plugins List all available plugins\n-muta
te+ Guess additional file names\n-mutate-options+ Provide extra information for mutations\n-output+ Write output to this file\n-nocache Disables the URI cache\n-nossl
Disables using SSL\n-no404 Disables 404 checks\n-Plugins List of plugins to run (default ALL)\n-port+ Port to use (default 80)\n-Display+ Turn on/off
display outputs\n-ssl Force ssl mode on port\n-Single Single request mode\n-timeout+ Timeout (default 2 seconds)\n-Tuning+ Scan tuning\n-update Upd
ate databases and plugins from cirt.net (cannot be abbreviated)\n-Version Print plugin and database versions\n-vhost+ Virtual host (for Host header)\n+ requires a value\n\n\n
results|163.10.10|163.10.10.109|general/HOST-T|1.3.6.1.4.1.25623.1.0.810003|Log Message|traceroute:163.10.20.60,163.10.20.1,163.10.33.189,163.10.33.54,* * *,163.10.10.109\nports:\n\n
results|163.10.10|163.10.10.109|general/tcp|1.3.6.1.4.1.25623.1.0.19506|Log Message|Information about this scan : \n\nOpenVAS version : 3.1.3.\nPlugin feed version : 201011171340\nType of plugin feed : OpenV
AS NVT Feed\nScanner IP : 163.10.20.60\nPort range : 1-65535\nThorough tests : no\nExperimental tests : no\nParanoia level : 1\nReport Verbosity : 1\nSafe checks : yes\nMax hosts : 30\nMax checks : 10\nScan
Start Date : 2010/12/3 7:37\nScan duration : 14238 sec\n\n
results|163.10.10|163.10.10.109|general/CPE|1.3.6.1.4.1.25623.1.0.810002|Log Message|No CPE identities could be determined.\n
timestamps||163.10.10.109|host_end|Fri Dec 3 11:34:38 2010|
timestamps|||scan_end|Fri Dec 3 11:34:38 2010|
```



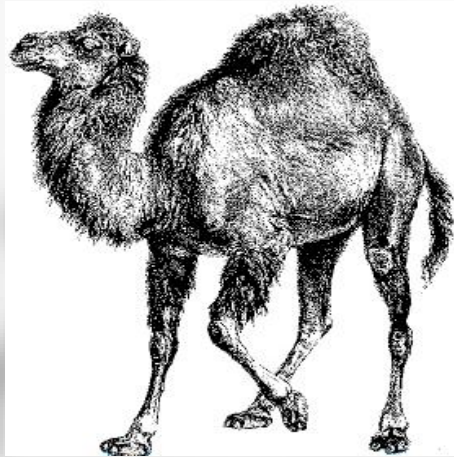
# El producto

- **¿Qué buscamos?**
  - Integrar las herramientas con el fin de que lo que una produzca lo pueda utilizar el resto.
  - Unificar y congrega los resultados y la administración de cada una de estas herramientas
  - **SIMPLIFICAR !!!!!!!**
    - **AHORRAR RECURSOS**
    - **DETECTAR Y MINIMIZAR ERRORES**
    - **DETECTAR Y RESPONDER RAPIDAMENTE A EVENTOS**

# El producto final



# El producto final



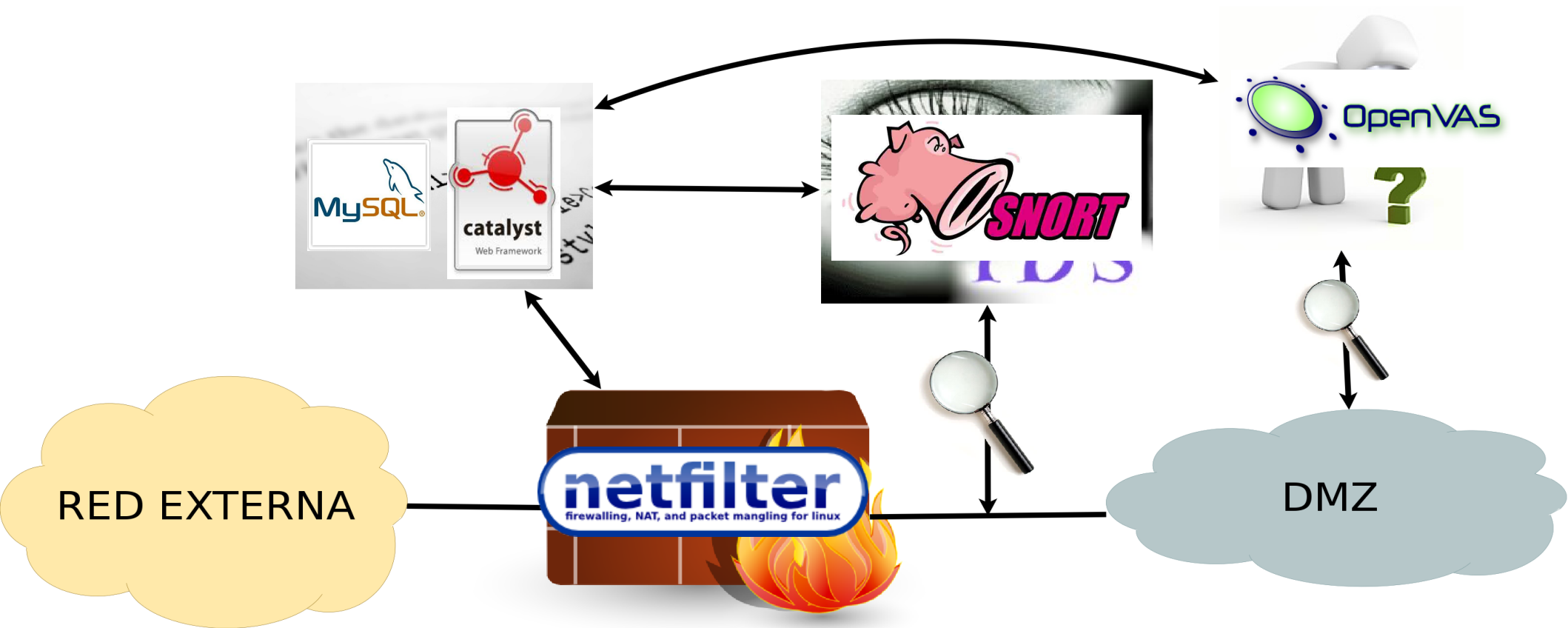
# El producto final

- Respeta Model View Controller
- Dont Repeat Yourself
- Desarrollo Orientado a Objetos
- Aprueba validaciones de W3C (XHTML 1.0 Strict y CSS 2.1)
- Desarrollo distribuido usando Subversion

# El producto final


- Algunas cifras sobre el trabajo realizado:
  - Más de 350 commits al repositorio
  - Cerca de 3000 líneas de código
  - Unos 100 archivos diferentes
  - 82 clases
  - 39 tablas en la base de datos

# Producto final - Funcionamiento











# Integración del Firewall:

- Tráfico a un servidor:


Tráfico: Sitio Web Linti (163.10.10.13/255.255.255.255) 

Tráfico Entrante →


PROTOCOLO	PUERTO	IP ORIGEN	MASCARA ORIGEN	ESTADO	HABILITADO	ACCION
TCP	80	0.0.0.0	255.255.255.255	NEW		 
TCP	80	0.0.0.0	0.0.0.0	NEW, ESTABLISHED, RELATED		 
TCP	443	0.0.0.0	0.0.0.0	NEW, ESTABLISHED, RELATED		 

Tráfico Saliente ←

PROTOCOLO	PUERTO	IP DESTINO	MASCARA DESTINO	ESTADO	HABILITADO	ACCION
-----------	--------	------------	-----------------	--------	------------	--------

Tráfico Entrante Bloqueado → 

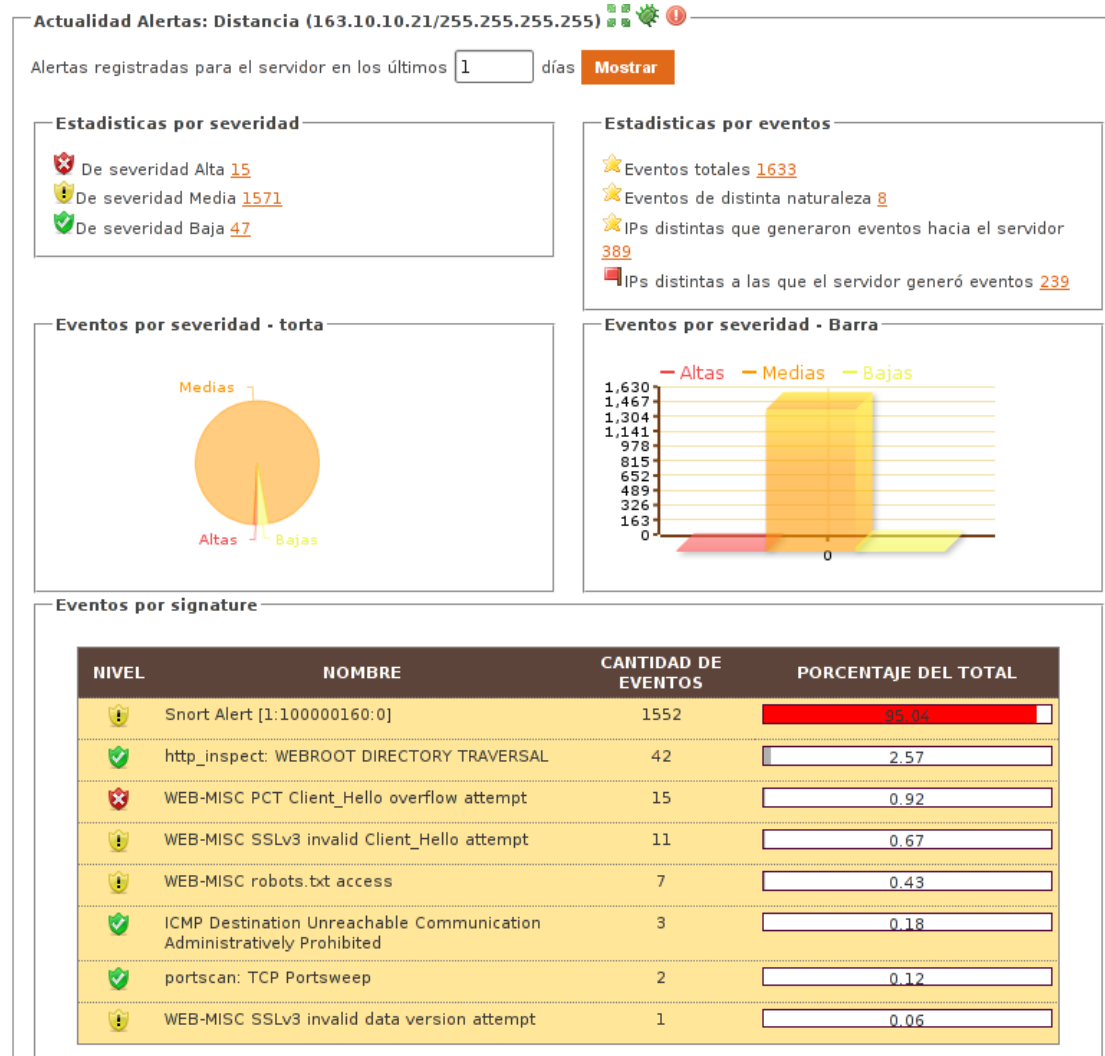
PROTOCOLO	PUERTO	IP ORIGEN	MASCARA ORIGEN	ESTADO	ACCION
-----------	--------	-----------	----------------	--------	--------

Tráfico Saliente Bloqueado ← 

PROTOCOLO	PUERTO	IP DESTINO	MASCARA DESTINO	ESTADO	ACCION
-----------	--------	------------	-----------------	--------	--------

# Integración del IDS:

- Alertas de un servidor:





# Integración del Escaner de Vulnerabilidades:

- Reporte de escaneo :

## Resultado de Escaneo

Actualidad Escaneo: Sitio Web Linti (163.10.10.13/255.255.255.255)

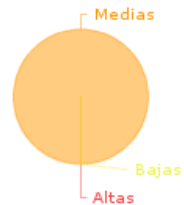
### Detalle

Servidor: 163.10.10.13/255.255.255.255  
Frecuencia: **Diario**  
Estado: **Fin**  
Último Escaneo: **06/12/2010**

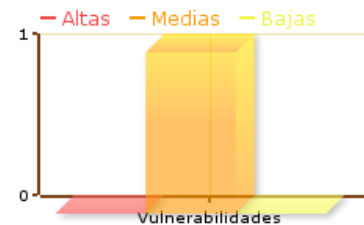
### Estadísticas por severidad

De severidad Alta 0  
 De severidad Media 1  
 De severidad Baja 0

### Vulnerabilidades por severidad - Torta



### Vulnerabilidades por severidad - Barras



### Resultado del Último Escaneo (06/12/2010)

IP	PUERTO	OID	TIPO	RIESGO	CVE		
DE SEVERIDAD MEDIA							
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.100153	Security Warning	Medium	CVE-2008-5161		+
INFORMACIÓN							
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.50282	Log Message	None			+
163.10.10.13	http (80/tcp)	1.3.6.1.4.1.25623.1.0.10386	Security Note	None			+
163.10.10.13	general/tcp	1.3.6.1.4.1.25623.1.0.80091	Security Note	None			+
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.100259	Security Note	None			+
163.10.10.13	ssh (22/tcp)	1.3.6.1.4.1.25623.1.0.10330	Security Note	-			+
163.10.10.13	http (80/tcp)	1.3.6.1.4.1.25623.1.0.10330	Security Note	-			+
163.10.10.13	https (443/tcp)	1.3.6.1.4.1.25623.1.0.10330	Security Note	-			+

# Trabajos a Futuro

- Retribuir a la comunidad del software libre
- ~~Instalar el software en un ambiente producción~~
- Mejorar la documentación
- Empaquetar la aplicación para facilitar su distribución
- ~~Desarrollar una guía de instalación.~~
- ~~Agregar la posibilidad de reglas por defecto para el Firewall~~
- Mejorar la parte de auditoría del sistema
- Exportar alertas del Snort y resultados de escaneos a varios formatos
- Subir reportes de escaneos antiguos con fines estadísticos
- Desarrollar un módulo de reportes vía mail
- Agregar el soporte para IPV6.
- Agregar la posibilidad de utilizar múltiples IDS

# Ambiente en producción

DEMO!!!!

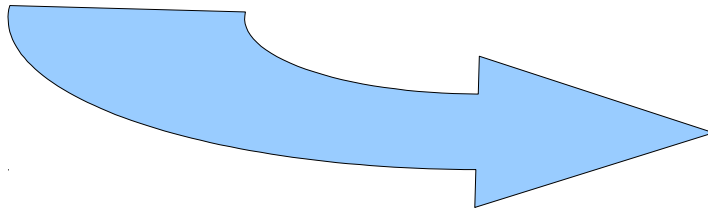
# Conclusiones

- El software que planteamos inicialmente como un prototipo hoy es un sistema puesto en producción en un ambiente real.
- No es necesario ser un experto para manejar el sistema.
- El sistema integra eficazmente herramientas de distinta naturaleza cubriendo casi todas las capas del modelo TCP-IP.
- Respeta los estándares de desarrollo web de la W3C y sigue buenas técnicas de programación como MVC y DRY.

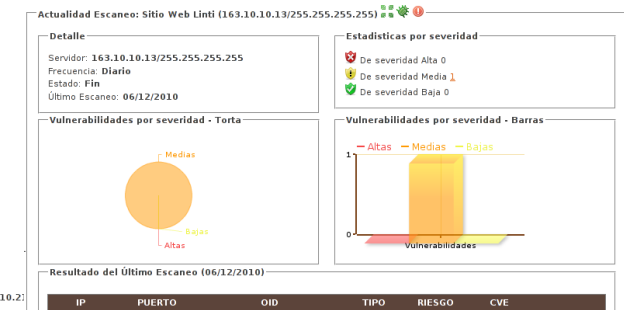
# Conclusiones

- Consideramos que el texto resultante es un buen punto de partida para introducirse en los temas de seguridad involucrados.
- El trabajo se realizó íntegramente utilizando aplicaciones de Software Libre, desde la propuesta hasta el desarrollo de esta presentación.

# ¿Preguntas?



## Resultado de Escaneo



Actualidad Alertas: Distancia (163.10.10.2)

Alertas registradas para el servidor en los últimos

**Estadísticas por severidad**  
De severidad Alta 15  
De severidad Media 1571  
De severidad Baja 47

**Eventos por severidad - torta**

**Eventos por signature**

NIVEL	HOMBRE	CAN	EN
1	Snort Alert [1.100000160:0]		
2	http_inspect: WEBROOT DIRECTORY TRAVERSAL		
3	WEB-MISC PCT_Client_Hello overflow attempt		
4	WEB-MISC SSLv3 invalid Client_Hello attempt		
5	WEB-MISC robots.txt access		
6	ICMP Destination Unreachable Communication Administratively Prohibited		
7	portscan: TCP Portswep		
8	WEB-MISC SSLv3 invalid data version attempt		

## Servidor Tesis

Usuarios Mis Datos Servidores Escaneos Preferencias Ayuda

Bienvenido Diego Maradona Salir Buscar servidor:

**Tráfico: Servidor Windows (192.168.56.101/255.255.0)**

**Tráfico Entrante**

PROTOCOLO	PUERTO	IP ORIGEN	MASCARA ORIGEN	ESTADO	HABILITADO	ACCION
UDP	111	10.0.0.1	255.255.255.0	RELATED		
TCP	80	163.10.10.99	255.255.255.192	NEW, ESTABLISHED, RELATED		

**Tráfico Saliente**

PROTOCOLO	PUERTO	IP DESTINO	MASCARA DESTINO	ESTADO	HABILITADO	ACCION
UDP	121	190.0.0.1	255.255.255.192	RELATED		
ICMP	11	222.222.222.222	255.0.0.0	RELATED		
TCP	123	192.168.56.101	255.255.255.0	RELATED		
TCP	123	192.168.56.101	255.255.255.0	RELATED		

**Tráfico Entrante Bloqueado**

PROTOCOLO	PUERTO	IP ORIGEN	MASCARA ORIGEN	ESTADO	ACCION
-----------	--------	-----------	----------------	--------	--------

**Tráfico Saliente Bloqueado**

PROTOCOLO	PUERTO	IP DESTINO	MASCARA DESTINO	ESTADO	ACCION
-----------	--------	------------	-----------------	--------	--------